CHRISTOPHER W. JAMES (SBN 289047)
cjames@velaw.com
VINSON & ELKINS LLP
350 South Grand, Suite 2100
Los Angeles, CA 90071
555 Mission Street, Suite 2000
San Francisco, California 94105
Telephone: 415.979.6949
Facsimile: 415.520.5989

EPHRAIM WERNICK (admitted *pro hac vice*)
ewernick@velaw.com
VINSON & ELKINS LLP
2001 Ross Avenue, Suite 3900
Dallas, Texas 75201
Telephone: 202.639.6730
Facsimile: 202.879.8830

BRIANA R. FALCON (admitted *pro hac vice*)
bfalcon@velaw.com
VINSON & ELKINS LLP
845 Texas Avenue, Suite 4700
Houston, Texas 77002
Telephone: 713.758.2383
Facsimile: 713.615.5735

Attorneys for Defendant MoneyGram Payment Systems, Inc.

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

JOSE GUZMAN, FORTINO RUTILO JIMENEZ, BERTHA MEZA, GRISELDA AVILES CARRILLO and JOSE GERARDO VALLEJO PEREZ individually and on behalf of all others similarly situated,

Plaintiffs.

v.

WESTERN UNION FINANCIAL SERVICES, INC., MONEYGRAM PAYMENT SYSTEMS, INC., DOLEX DOLLAR EXPRESS, INC. and FORCEPOINT, LLC.

Defendants.

Case No.: 5:24-cv-404

MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF ALL DEFENDANTS' JOINT MOTION TO DISMISS FIRST AMENDED COMPLAINT

Date: March 21, 2024
Time: 2:00 p.m.
Location: Courtroom 2
Judge: Hon. Sunshine S. Sykes

Trial Date: None Set
Date Action Filed: February 21, 2024
First Am. Comp. Filed: April 21, 2024

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

Other Authorities

I. INTRODUCTION

This action should be dismissed pursuant to both Rules 12(b)(7) and 12(b)(6). Plaintiffs' entire First Amended Complaint ("FAC") is premised on money transfer businesses' production of money transfer records pursuant to compulsory administrative subpoenas. The Arizona Attorney General and the State of Arizona have claimed an interest in this litigation, and the Court cannot issue a ruling for Plaintiffs without impairing Arizona's interests and/or leaving the money transfer businesses subject to inconsistent obligations. The Arizona Attorney General and the State of Arizona are thus required parties that cannot be joined, so this action must be dismissed under Rule 12(b)(7). Additionally, because the money transfer business defendants produced records in response to subpoenas, they are immune from liability under the Annunzio-Wylie Anti-Money Laundering Act of 1992 (the "Annunzio-Wylie Act"). Plaintiffs' misapplied California Consumer Privacy Protection Act ("CCPA") claim fails both under a similar exception for responses to government subpoenas, and because the CCPA's private right of action applies only to disclosures resulting from security failures. And the California Constitution claim suffers basic pleading deficiencies, and otherwise fails to clear the high bar required to allege an expectation of privacy or an egregious breach of social norms for disclosures made in the context of a response to government subpoenas.

Defendants in this case are three money transfer businesses, Western Union Financial Services, Inc. ("Western Union"), MoneyGram Payment Systems, Inc. ("MoneyGram"), and DolEx Dollar Express, Inc. ("DolEx") (collectively, the "MTB Defendants"), as well as a cybersecurity software vendor, Forcepoint LLC ("Forcepoint"). Plaintiffs' FAC alleges that Defendants violated the CCPA and committed an invasion of privacy in violation of Article 1, Section 1 of the California Constitution. Plaintiffs' claims are based on the MTB Defendants' productions of certain money transfer records made in response to compulsory administrative

subpoenas issued by the Arizona Attorney General and Homeland Security Investigations ("HSI"), and Forcepoint's role in maintaining the database that houses the productions. Plaintiffs essentially claim that the MTB Defendants should have refused to comply with the subpoenas. They seek a ruling from this Court enjoining the MTB Defendants from continued compliance with subpoenas from the Arizona Attorney General, declaring that the MTB Defendants' compliance with the subpoenas is unlawful, and awarding exorbitant money damages.

Plaintiffs are not the first consumers to sue money transfer businesses for alleged violations of California law based on their compliance with Arizona Attorney General and HSI subpoenas. In *Sequeira v. United States Department of Homeland Security et al.*, No. 22-cv-07996-HSG (N.D. Cal.), a different set of plaintiffs sued three money transfer businesses—including Western Union and DolEx—based on identical factual allegations. After the Arizona Attorney General expressed her interest in the case, the court dismissed the action under Federal Rules of Civil Procedure 12(b)(7) and 19, holding that "joinder of Arizona is both necessary and not feasible, and the case cannot proceed in equity and good conscience without Arizona." *Sequeira*, 2024 WL 4351137, at *5 (N.D. Cal. Sept. 30, 2024).

This Court should reach the same conclusion and dismiss this action under Rules 12(b)(7) and 19. As in *Sequeira*, the State of Arizona and Arizona Attorney General have claimed an interest in this litigation as set forth in Arizona Attorney General Kris Mayes's letter to the Court. Declaration of Sheila A.G. Armbrust in support of Defendants' Motion to Dismiss FAC ("Armbrust Decl."), Ex. 6 at 42-43. General Mayes observes that "it is difficult to identify a party more interested in [this] litigation than the State of Arizona." *Id.* at 43. Among other things, she explains that her success in combatting transnational criminal organizations "is highly dependent on [her] ability to issue and enforce the subpoenas and obtain the requested transactional records that are at the crux of the present matter." *Id.* As in *Sequeira*, the resolution of Plaintiffs'

claims without the State of Arizona and the Arizona Attorney General could both impair Arizona's interest in compliance with its subpoenas and leave the MTB Defendants stuck "between the proverbial rock and a hard place" (either refuse to comply with the subpoenas and be prosecuted or held in contempt, or comply with the subpoenas and face civil liability and exorbitant damages). 2024 WL 4351137, at *4–5. As in *Sequeira*, the State of Arizona and the Arizona Attorney General cannot be joined because they enjoy sovereign immunity. *Id.* at 5. And as in *Sequeira*, the case cannot move forward in equity and good conscience without the State of Arizona and the Arizona Attorney General. *Id*. The Court therefore should dismiss the action under Rules 12(b)(7) and 19 for failure to join required parties.

The FAC should also be dismissed under Rule 12(b)(6) for failure to state a claim for a number of different reasons. To begin, both of Plaintiffs' claims are barred by the Annunzio-Wylie Act. The Annunzio-Wylie Act expressly immunizes financial institutions such as the MTB Defendants from liability for disclosures of money transfer records made pursuant to legal authority, such as subpoenas. Plaintiffs' attempt to assert that the subpoenas at issue here were invalid—and that the MTB Defendants knew that the subpoenas were invalid—based on an old, distinguishable case from 2007 does not save their claims.

Plaintiffs' CCPA claim fails for two additional, independent reasons. First, the only private right of action under that statute concerns data breaches, Cal. Civ. Code § 1798.150, but Plaintiffs do not allege one here. To the contrary, Plaintiffs attack the production of money transfer records pursuant to subpoenas. Second, the CCPA contains an express exemption for compliance with a "civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities." Cal. Civ. Code § 1798.145. In other words, the statute itself recognizes that productions made pursuant to a subpoena do not give rise to liability under the CCPA.

Finally, Plaintiffs' invasion of privacy claim under the California Constitution is equally flawed. Such claims are held to a high bar, and Plaintiffs' allegations fail to establish any of the required elements. First, Plaintiffs fail to plead that the MTB Defendants produced the type of data that courts recognize is subject to a legally protected privacy interest. Second, Plaintiffs had no reasonable expectation of privacy in the transactional data that the MTB Defendants produced, including because Plaintiffs provided their transactional data to the MTB Defendants subject to transactional reporting laws, and did so while on express and repeated notice that the MTB Defendants might produce their data to law enforcement. Third, Plaintiffs cannot allege that the MTB Defendants' compliance with law enforcement subpoenas is sufficiently serious to constitute a breach of social norms, let alone an "egregious" breach as required to constitute a constitutional violation. Indeed, courts regularly hold that governmental functions—like compliance with law enforcement subpoenas—justify such disclosures, even where there may be a privacy interest.

For the aforementioned reasons, as explained more fully below, the FAC should be dismissed with prejudice.

II. BACKGROUND

The MTB Defendants are "in the business of providing money transfer services to individual consumers, typically across international borders." FAC ¶ 1. Plaintiffs allege that they were customers of the respective MTB Defendants and used their services to send money from California to Mexico: (i) Guzman (in 2020) and Meza (in 2022) allege they transacted through Western Union; (ii) Jimenez (in 2022) alleges he transacted through MoneyGram; and (iii) Carillo (in 2022) and Perez (in 2020 and 2022) allege they transacted through DolEx. *Id.* ¶¶ 116–20.

Plaintiffs' claims that Defendants violated the CCPA and California Constitution are premised entirely on the MTB Defendants' production of their money transfer records between 2020 and 2022 to state and federal law enforcement. *Id.* Notably,

Plaintiffs expressly allege that the MTB Defendants produced these records in response to compulsory process—namely, administrative subpoenas from the Arizona Attorney General and customs summonses, a form of administrative subpoena, from HSI. *See id.* ¶¶ 45, 48, 59–60, 62–65. Plaintiffs also allege that each of the MTB Defendants continues to disclose money transfer records to state law enforcement today. *Id.* ¶¶ 52, 70.

Plaintiffs incorporated into the FAC an exemplar subpoena issued to MoneyGram, which Plaintiffs excerpted in the FAC and attached to the FAC in full as Exhibit A. FAC ¶ 60; Dkt. 30-1 (Ex. A to FAC). The subpoena is signed by the Assistant Attorney General of the Arizona Attorney General's Office, carries the seal of the Attorney General, states that it was issued "in connection with the lawful performance of [] official duties as an Assistant Attorney General of the State of Arizona," cites the relevant Arizona statutory authority, and states that the subpoena was issued pursuant to a "felony investigation" to "investigate racketeering" activity. Dkt. 30-1 (Ex. A. to FAC) at 1–2. The subpoena "command[s]" MoneyGram to produce certain "described records," requires that the demanded data "be delivered electronically to the Arizona Attorney General's Office," and directs questions to an Arizona Attorney General investigator. *Id.* An individual affiliated with Forcepoint is identified to provide "the secure VPN address" and data formatting assistance, and is identified as the Arizona Attorney General Office's "agent." *Id.* at 2. And the subpoena threatens enforcement proceedings for failure to comply. *Id.*

Plaintiffs allege that the money transfer records produced by the MTB Defendants pursuant to the Arizona Attorney General and HSI subpoenas were sent to the Transactional Record Analysis Center ("TRAC"). FAC ¶ 5. TRAC, in turn, provided access to the money transfer records to law enforcement agencies, including the Arizona Attorney General. *Id.* ¶ 8.

TRAC was created in 2014 as part of an amendment to a 2010 settlement between Western Union and the Arizona Attorney General. *Id.* ¶ 35(b). The settlement followed years of litigation originally arising out of 2006 subpoenas issued to Western Union by the Arizona Attorney General, which sought data related to "transaction[s] of $300 and greater received in the state of Sonora, Mexico … beginning with January 1, 2004, and ending with December 31, 2006." *Id.* ¶ 30. Western Union "fought the enforcement of the subpoenas," *id.* ¶ 31, and in *State ex rel. Goddard v. W. Union Fin. Servs., Inc.*, the Arizona Court of Appeals issued a narrow holding, recognizing that "law-enforcement agencies may want to 'keep ahead' of the traffickers who, in the relatively mobile and global world of money transfer, may have the ability to quickly adjust where and how they transfer racketeering proceeds," but concluding that the breadth of the particular subpoena before it "was not reasonable in light of the justification offered for it." 166 P.3d 916, 926–27 (Ariz. Ct. App. 2007).

TRAC was initially funded by the Arizona Financial Crimes Task Force ("AZFCTF"). FAC ¶ 80; *see also* Dkt. 30-2 (Ex. B to FAC) at 1; *Sequeira*, 2024 WL 4351137, at *1 (TRAC "was founded … by the [AZFCTF]—comprising the Arizona Attorney General's Office, Phoenix Police Department, and Arizona Department of Public Safety, with the participation of DHS."). The AZFCTF "was established to investigate and interdict the money laundering activities of complex national and international organized crime and to mitigate the violence associated with the smuggling activities that fund these organizations." Dkt 30-2 (Ex. B to FAC) at 1. TRAC "serves as the intelligence component for AZFCTF and is staffed by analyst and law enforcement professionals recognized as experts in money laundering activity." *Id.* "TRAC provides data, meaningful data analysis, collaboration and training to investigators, analysts and prosecutors nationwide in their efforts to disrupt criminal organizations and dismantle their operations." *Id.*

The AZFCTF engaged Defendant Forcepoint as a software vendor for the TRAC database, providing analytics and data management solutions for the incoming data. FAC ¶¶ 79, 82. Forcepoint is alleged to have provided the AZFCTF with a "specifically tailored" and "customized" technical solution to permit access to the specified law enforcement community "while preserving the custody, security and physical ownership of the data." *Id.* ¶¶ 82, 97. Indeed, the TRAC Data Policy is clear that law enforcement can use the TRAC database only if "consistent with their legal authority, only on a need-to-know basis, and only for the identification, investigation, or prosecution of reasonably possible or actual violations of law." Dkt. 30-4 (Ex. D to FAC) at 4–5. Forcepoint did not have any responsibility, authority, or control over how that data was used or shared, nor is Forcepoint alleged to have determined or controlled whether or to what agencies are granted access to the TRAC database.

III. LEGAL STANDARD

A Rule 12(b)(7) motion to dismiss is premised on the failure to join a required party under Rule 19. A court should grant a motion to dismiss for failure to join a required party where the absent party is necessary to the action but cannot be joined, so that in equity and good conscience the suit must be dismissed. Fed. R. Civ. P. 19.

Dismissal is appropriate under Rule 12(b)(6) "where the complaint lacks a cognizable legal theory or sufficient facts to support a cognizable legal theory." *Mendiondo v. Centinela Hosp. Med. Ctr.*, 521 F.3d 1097, 1104 (9th Cir. 2008). A complaint that does not "contain sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face" will not survive a motion to dismiss. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quotations omitted). Further, conclusory allegations are not entitled to a presumption of truth on a motion to dismiss, and a plaintiff "armed with nothing more than conclusions" or "[t]hreadbare recitals of the elements of a cause of action" fails to state a claim. *Id.* at 678–81.

When ruling on a Rule 12(b)(6) motion, the Court may consider the facts alleged in the pleading, documents incorporated into the pleading by reference, and documents subject to judicial notice. *See* Fed. R. Evid. 201; *Khoja v. Orexigen Therapeutics, Inc.*, 899 F.3d 988, 999 (9th Cir. 2018). Documents incorporated by reference are treated as "part of the complaint, and thus [the Court] may assume that [their] contents are true for purposes of a motion to dismiss under Rule 12(b)(6)." *Marder v. Lopez*, 450 F.3d 445, 448 (9th Cir. 2006) (citing *United States v. Ritchie*, 342 F.3d 903, 908 (9th Cir. 2003)). The Court need not accept as true complaint allegations that "contradict matters properly subject to judicial notice" or that "conflict with" documents "incorporated by reference into the complaint." *Gonzalez v. Planned Parenthood of L.A.*, 759 F.3d 1112, 1115 (9th Cir. 2014) (citations omitted).[1]

IV. ARGUMENT

A. The Action Should Be Dismissed Under Rule 12(b)(7) Because The State Of Arizona And The Arizona Attorney General Are Required Parties Who Cannot Be Joined.

Under Federal Rule of Civil Procedure 19, a non-party to an action "must be joined as a party," if feasible, if that person (1) "claims an interest relating to the subject of the action" and (2) "disposing of the action in the person's absence may" (i) "impair or impede the person's ability to protect the interest," or (ii) "leave an existing party subject to a substantial risk of ... inconsistent obligations because of the interest." Fed. R. Civ. P. 19(a)(1)(B). If an otherwise required party "cannot be joined"—for example, if they enjoy sovereign immunity—"the court must determine whether, in equity and good conscience, the action should proceed among the existing parties or should be dismissed." Fed. R. Civ. P. 19(b).

[1] Defendants have submitted an accompanying Request for Judicial Notice concerning various exhibits either attached to accompanying declarations in support of this Motion to Dismiss, or previously submitted in this matter. *See* All Defendants' Request for Judicial Notice in Support of Motion to Dismiss FAC ("RJN"), filed herewith.

As the court in *Sequeira* recently held in connection with virtually identical factual allegations related to the production of money transfer records to TRAC, the State of Arizona and the Arizona Attorney General are required parties to this action who cannot feasibly be joined because they enjoy sovereign immunity, and in equity and good action, this action cannot proceed without them. 2024 WL 4351137, at *3–5. Accordingly, the action should be dismissed.

1. The State Of Arizona And The Arizona Attorney General Are Required Parties.

The State of Arizona and the Arizona Attorney General are required parties under Rule 19(a)(1)(B) because they claimed an interest in this action, and resolving this action in their absence would both impede their ability to protect their law enforcement interests and pose a risk that the MTB Defendants would face inconsistent obligations.

On November 14, 2024, the current Arizona Attorney General, Kris Mayes, submitted a letter to the Court stating Arizona's interest. Armbrust Decl., Ex. 6 at 42-43; *see also* Armbrust Decl., Ex. 7 at 54-64 (attaching Arizona Attorney General Strategy Memo). General Mayes explained that "Representatives from [her] office are closely monitoring [the] progress" of this case, and that "the State of Arizona and [Mayes], in [her] official capacity as the Arizona Attorney General, are highly vested in the outcome of this matter." *Id.* at 1. Specifically, the Arizona Attorney General has "been steadfast in [her] commitment to tackling the evils committed by Transnational Criminal Organizations (TCOs) operating in the Southwest Border area" and has "embraced and furthered a program first implemented by a preceding Arizona Attorney General targeting these organizations' laundering of illicit proceeds through Money Service Businesses (MSBs)." *Id.* at 1–2. The Arizona Attorney General's "success in combatting these sophisticated TCOs is highly dependent on [her] ability to issue and enforce the subpoenas and obtain the requested transactional records that are at the crux of the present matter." *Id.* at 2. General Mayes concluded: "Because a primary issue

before this Court is the legality of the Defendant MSBs' compliance with these subpoenas, I believe it is important to notify this Court of the State of Arizona's interest in this matter," and "it is difficult to identify a party more interested in such litigation than the State of Arizona." *Id.* Unquestionably, by submitting this letter, the Arizona Attorney General and the State of Arizona have "claimed an interest in the subject matter of this litigation, such that Rule 19([a])(1)(B) applies." *Sequeira*, 2024 WL 4351137, at *3.

Additionally, even prior to the Arizona Attorney General's letter, the Arizona Attorney General and the State of Arizona had already claimed an interest in this matter consistent with Rule 19(a)(1)(B), because "[a] public entity has an interest in a lawsuit that could result in the invalidation or modification of one of its ordinances, rules, regulations, or practices." *EEOC v. Peabody Western Coal Co.*, 610 F.3d 1070, 1082 (9th Cir. 2010). This is true even where the public entity does not take any explicit step to state its interest in the litigation. *See id.*; *see also, e.g.*, *Linehan v. Allianceone Receivables Mgmt., Inc.*, No. C15-1012-JCC, 2016 WL 4765839, at *9 (W.D. Was. Sept. 13, 2016) ("The *Peabody* court reached this conclusion despite the fact the public entity in that case did not explicitly claim an interest in the litigation."); *Tinoco v. San Diego Gas & Elec. Co.*, 327 F.R.D. 651, 659 (S.D. Cal. Sept. 6, 2018) (explaining that in *Peabody*, "[i]t did not appear the person to be joined (the Secretary of the Interior) had claimed an interest in the lawsuit, but the Ninth Circuit held he was to be joined because the action 'would require him to modify the terms of leases he approves for [certain] entities.'" (quoting *Peabody*, 610 F.3d at 1082)); *Cal. Dump Truck Owners Ass'n v. Nichols*, 924 F. Supp. 2d 1126, 1147–48 (E.D. Cal. 2012).

Next, as the court held in *Sequeira*, both Rules 19(a)(1)(B)(i) and 19(a)(1)(B)(ii) are separately applicable. *First*, if this case were to go forward without the State of Arizona and the Arizona Attorney General, disposing of the action may impair or impede the State of Arizona and Arizona Attorney General's ability to protect their

interests. Fed. R. Civ. P. 19(a)(1)(B)(i). Plaintiffs seek both injunctive relief and a declaration that the MTB Defendants' compliance with the subpoenas is unlawful. FAC ¶ 128; *see also id.* at p. 43 (Prayer For Relief at (b), (d), and (i)). "Arizona has a legally protected interest in Money Transfer Defendants' full compliance with its subpoenas, including regulating disclosures about the investigations in which they are issued." *Sequeira*, 2024 WL 4351137, at *5. "If this Court were to award Plaintiffs injunctive relief, ... it would materially impact that interest." *Id.* Moreover, as in *Sequeira*, Plaintiffs here alleged that the Arizona subpoenas are "overbroad and 'invalid.'" *Id.*; *see, e.g.*, FAC ¶¶ 6–7, 46–48, 55, 67–68, 73. This "only further confirms that any ruling for Plaintiffs on the merits in this case will necessarily implicate and impair Arizona's legally protected interests"—defending the Arizona Attorney General's subpoenas. *Sequeira*, 2024 WL 4351137, at *5; *see also Peabody*, 610 F.3d at 1081–82 ("If the Secretary is not joined, he will be unable to defend his interest in the legality of the lease provision.").

Second, if this case were to proceed without the State of Arizona and the Arizona Attorney General, the MTB Defendants would face a risk of inconsistent obligations—being forced to choose between complying with the Arizona Attorney General's subpoenas or a potential order of this Court declaring the subpoenas unlawful. *See* Fed. R. Civ. P. 19(a)(1)(B)(ii). "[I]f this Court were to award money damages to Plaintiffs, it would be doing so based on a finding that Money Transfer Defendants' conduct in producing financial records was illegal." *Sequeira*, 2024 WL 4351137, at *4. "If that happened, going forward, Money Transfer Defendants would be forced either to refuse to comply with further subpoenas from Arizona, or to continue to engage in conduct that this Court had found to violate" the applicable California law. *Id.* As a result, the "Money Transfer Defendants would be stuck 'between the proverbial rock and a hard place' of either refusing to comply with Arizona's subpoenas or violating" California law. *Id.* (quoting *Dawavendewa v. Salt River Project Agric. Imp. & Power Dist.*, 276

F.3d 1150, 1156 (9th Cir. 2002)); *see also Peabody*, 610 F.3d at 1082 (holding the Secretary of the Interior is a required party under Rule 19(a)(1)(B)(ii) because "[i]f the Secretary is not made a party and if EEOC prevails, the Secretary may choose to ... continue the leases in the current form, ignoring the judgment in the case to which he was not made a party. If the Secretary chooses to do this, he will put [the defendant] 'between the proverbial rock and a hard place'" (citation omitted)); *id.* at 1080 ("The central problem is that [the defendant] is caught in the middle of a dispute not of its own making.").

2. The State of Arizona And The Arizona Attorney General Cannot Be Joined In This Action.

Under the Eleventh Amendment, a state is "immune from suits brought in federal courts by her own citizens as well as by citizens of another state." *Pennhurst State School & Hosp. v. Halderman*, 465 U.S. 89, 100 (1984) (citation omitted); *see also Dittman v. Cal.*, 191 F.3d 1020, 1025 (9th Cir. 1999) ("[U]nder the Eleventh Amendment, agencies of the state are immune from private damages actions or suits for injunctive relief brought in federal court." (citation omitted)). Accordingly, as in *Sequeira*, the State of Arizona and the Arizona Attorney General enjoy Eleventh Amendment sovereign immunity and cannot be joined in this case. *See* 2024 WL 4351137, at *5.

3. The Case Should Be Dismissed Because It Cannot Proceed In Equity And Good Conscience In The Absence Of The State Of Arizona And The Arizona Attorney General.

Under Rule 19(b), the Court must consider the following factors to determine whether this action can proceed, "in equity and good conscience," without Arizona and the Arizona Attorney General as parties:

> (1) the extent to which a judgment rendered in the person's absence might prejudice that person or the existing parties;
> (2) the extent to which any prejudice could be lessened or avoided by:

> (A) protective provisions in the judgment;
>
> (B) shaping the relief; or
>
> (C) other measures;
>
> (3) whether a judgment rendered in the person's absence would be adequate; and
>
> (4) whether the plaintiff would have an adequate remedy if the action were dismissed for nonjoinder.

Fed. R. Civ. 19(b).

The State of Arizona and the Arizona Attorney General are essential. As General Mayes explained, "[b]ecause a primary issue before this Court is the legality of the [MTB Defendants'] compliance with [the Arizona Attorney General's] subpoenas, ... it is difficult to identify a party more interested" in this litigation than Arizona and the Arizona Attorney General. Armbrust Decl., Ex. 6 at 43. Both the State of Arizona and the Arizona Attorney General would be prejudiced by a judgment in this action for the same reasons that they are required parties: they have an interest in exercising their investigatory and police authority and in the continued operation of TRAC. No protective provisions, shaping of relief, or other measures can mitigate that prejudice, as any decision in Plaintiffs' favor would impair their investigatory power and interest in TRAC. Nor would a judgment in their absence be adequate. As stated above, anything other than a complete rejection of Plaintiffs' claims will result in inconsistent obligations for the MTB Defendants and run roughshod over core sovereign police power interests of the State of Arizona and the Arizona Attorney General.

In short, as the court explained in *Sequeira*, "any ruling in Plaintiffs' favor in this action would either (1) be inequitable for Money Transfer Defendants as it would require them to comply with future Arizona subpoenas and orders while simultaneously paying money damages in perpetuity; (2) materially impair Arizona's legally-protected

interests in the enforcement of subpoenas and court orders, or (3) both." 2024 WL 4351137, at *5. This Court therefore should dismiss this case.

B. Both Counts Should Be Dismissed Under Rule 12(b)(6) Because The Annunzio-Wylie Act Precludes Civil Liability For Production Of Money Transfer Records Made Pursuant To Subpoenas.

The FAC also must be dismissed because the MTB Defendants' productions of money transfer records pursuant to subpoenas are protected by the safe harbor in the Annunzio-Wylie Act 31 U.S.C. § 5318(g)(3)(A). The Annunzio-Wylie Act states that "financial institutions"—including money transmitters such as the MTB Defendants, 31 U.S.C. § 5312(a)(2)—are immune from civil liability for disclosures made pursuant to legal authority, which includes subpoenas. In relevant part, the Annunzio-Wylie Act provides:

> Any financial institution that makes a voluntary disclosure of any possible violation of law or regulation to a government agency ***or makes a disclosure pursuant to this subsection or any other authority … shall not be liable*** to any person under any law or regulation of the United States, any constitution, law, or regulation of any State or political subdivision of any State ... for such disclosure or for any failure to provide notice of such disclosure to the person who is the subject of such disclosure or any other person identified in the disclosure.

31 U.S.C. § 5318(g)(3)(A) (emphasis added). Courts have clarified that "any other authority" (which courts refer to as the Annunzio-Wylie Act's "third safe harbor") extends to disclosures made pursuant to any "legal authority," including any "statute, regulation, court order, or other source of law," including subpoenas. *Lopez v. First Union Nat'l Bank of Fla.*, 129 F.3d 1186, 1193–94 (11th Cir. 1997); *see also, e.g.*, *Coronado v. Bank Atl. Bancorp, Inc.*, 222 F.3d 1315, 1320 (11th Cir. 2000) (concluding that a grand jury subpoena—unlike a "mere verbal request from a government agent"—is considered "other authority," as subpoenas "possess the 'force of law' because they are issued under the authority of a federal district court, and disobedience can lead to a

legal sanction"); *Widi v. McNeil*, No. 2:12-cv-00188-JAW, 2013 WL 5407457, at *8 (D. Maine Sept. 25, 2013).

At bottom, the Annunzio-Wylie act reflects that a financial institution is "immune from any liability for any disclosures made pursuant to" subpoenas or other legal authority. *Lopez*, 129 F.3d at 1193–94. "Forcing a bank to challenge a facially valid [] subpoena in order to avoid liability to one (or more) of its customers would fly in the face ... of the Annunzio Wylie Act's clear intent to encourage cooperation" with government investigations. *Coronado*, 222 F.3d at 1321. And the broad protections provided by the Annunzio-Wylie Act apply in equal force to Plaintiffs' California law claims, as they state that financial institutions cannot be liable under *state law* for disclosures made pursuant to legal authority. *See* 31 U.S.C. § 5318(g)(3)(A).

Here, as Plaintiffs allege, the MTB Defendants' productions of money transfer records were made pursuant to subpoenas. *See, e.g.*, FAC ¶¶ 45, 48, 59–60, 62–65. These subpoenas fall within the "other authority" provision of the Annunzio-Wylie Act because they are legal authority. *See Lopez*, 129 F.3d at 1193–94; *Coronado*, 222 F.3d at 1320; *Widi*, 2013 WL 5407457, at *8.

Plaintiffs' repeated assertions that the MTB Defendants "knew" or "understood" that the subpoenas were "facially" unlawful, improper, invalid, or unenforceable, FAC ¶¶ 6–7, 46–48, 55, 67–68, 73, do not create an exception to the Annunzio-Wylie Act's third safe harbor. As a preliminary matter, the subpoenas are not facially invalid. Plaintiffs' FAC—including through its incorporation of an Arizona Attorney General subpoena to MoneyGram—affirmatively demonstrates the subpoenas' validity. In particular, the subpoena is signed by the Assistant Attorney General of the Arizona Attorney General's Office, carries the seal of the Attorney General, states that it was issued "in connection with the lawful performance of [] official duties as an Assistant Attorney General of the State of Arizona," cites the relevant Arizona statutory

authority, and states that the subpoena was issued pursuant to a "felony investigation" to "investigate racketeering" activity. Dkt. 30-1 (Ex. A. to FAC) at 1–2.

Moreover, the only support Plaintiffs cite for their allegation that the MTB Defendants knew or should have known that the subpoenas were invalid is the Arizona Court of Appeals' 2007 decision in *State ex rel. Goddard v. Western Union Financial Services, Inc.*, 166 P.3d 916 (Ariz. Ct. App. 2007). *See* FAC ¶¶ 6, 32, 46, 68. According to Plaintiffs, *Goddard* involved "virtually identical facts" as those at issue here, and the subpoenas at issue in this case are "just as invalid and illegal" as those in *Goddard*. *Id.* ¶¶ 6, 68. Not so. *Goddard* is a 17-year-old case that is factually distinguishable and says nothing about the validity of the present subpoenas.

At issue in *Goddard* was the validity of an Arizona Attorney General subpoena that directed Western Union to produce transaction records for "any wire-transfers" of or greater than $300 "to any location in Sonora, Mexico from any Western Union location worldwide for a three-year period." 166 P.3d at 917. *Goddard* expressly declined to address the constitutionality of the Arizona Attorney General's subpoena. *Id.* at 920 ("[W]e do not reach Western Union's constitutional arguments."). The court held only that an Arizona statute, A.R.S. §13-2315 (the same statutory authority invoked in the subpoenas at issue) was a valid source of subpoena power and required "that the Attorney General have reasonable grounds to believe that the information sought is relevant to an investigation of a crime defined as racketeering under Arizona law," with no requirement that the Attorney General identify a specific criminal act or transaction. *Id.* at 921–23. And the court determined, on the facts before it, that the "breadth" of the request at issue "was not reasonable in light of the justification offered for it." *Id.* at 927.

Critically, the court in *Goddard* "appreciate[d] that law-enforcement agencies may want to 'keep ahead' of the traffickers who, in the relatively mobile and global world of money transfer, may have the ability to quickly adjust where and how they

transfer racketeering proceeds." *Id.* at 926. And the court rejected as "overstated" Western Union's argument "that the Attorney General ha[d] no right to investigate wire transactions that occur entirely outside" of Arizona. *Id*.

Goddard therefore turned on a failure of proof by the Arizona Attorney General, after a detailed assessment of the underlying investigative purpose and needs—not on any determination that it would be facially unlawful for the Arizona Attorney General to obtain financial records from money transfer service providers, even those concerning out-of-state customers. *Id.* at 923 (finding that transfers from various "corridor states" outside of Arizona were in fact justified). That the Arizona Attorney General failed to establish the requisite factual basis for the investigation at issue in *Goddard* does not provide the current Plaintiffs with any ground to argue that the Arizona Attorney General lacked such a basis for the different investigations at issue here. Indeed, the FAC makes no factual allegations that cast doubt on Arizona's investigative need for the subpoenas issued from 2019-22, such that the parties (or Court) could even begin to analyze whether their scope is appropriate—Plaintiffs offer only conclusory statements that the subpoenas are facially invalid.[2] And the FAC certainly does not provide any basis for Plaintiffs to allege that the MTB Defendants knew or should have known that the subpoenas at issue in this case were somehow invalid, unlawful, or unenforceable.

Because Plaintiffs acknowledge that the productions at issue here were made pursuant to subpoenas, they fall within the Annunzio-Wylie Act's safe harbor. The MTB Defendants are thus immune from liability, and this action should be dismissed with prejudice.

[2] Moreover, with the issuing states and agencies absent from the litigation, there is not likely to be a sufficiently developed record for the Court to conduct such an analysis.

C. Plaintiffs' CCPA Claim Should Be Dismissed Under Rule 12(b)(6) For Failure To State A Claim.

1. The CCPA Provides A Private Right Action Only For Alleged Data Breaches.

The CCPA creates only a narrow private right of action for alleged data breaches. Plaintiffs' allegations do not concern any data breach or other security failure but rather the affirmative production of customer data pursuant to government subpoenas. The CCPA in no way contemplates a private right of action against a business for an affirmative, compelled production of transaction data in response to compulsory legal process, where no data breach or other security failure occurred, and where there is no suggestion the information was intercepted by an unintended recipient. Plaintiffs therefore cannot state a claim under the CCPA.

The only private right of action in the CCPA is in Section 1798.50, titled "Personal Information Security Breaches." Cal. Civ. Code § 1798.150. It provides for statutory damages only to consumers whose personal data "is subject to an unauthorized access and exfiltration, theft, or disclosure ***as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices*** appropriate to the nature of the information to protect the personal information." *Id.* § 1798.150(a)(1) (emphasis added). The CCPA is clear that this private right of action "shall apply only" to alleged violations of the "security breaches" provision of the CCPA, and "shall not be based on violation of any other section of [the CCPA]." *Id.* § 1798.150(c).

Courts therefore widely recognize that "[t]he CCPA ... allow[s] a private right of action ***only in the event of a security breach***." *Delgado v. Meta Platforms, Inc.*, 718 F. Supp. 3d 1146, 1155 (N.D. Cal. 2024) (emphasis added); *see also, e.g., Danfer-Klaben v. JPMorgan Chase Bank, N.A.*, No. SACV 21-262 PSG (JDEx), 2022 WL 3012528, at *7 (C.D. Cal. Jan. 24, 2022) (dismissing CCPA allegations that bank "allegedly continued to access and share Plaintiffs' personal information with

unspecified third parties for profit" because "Plaintiffs in no way allege that Defendants' disclosure to third parties was the result of a failure 'to implement and maintain reasonable security measures'" (citation omitted)); *Gershfeld v. Teamviewer US, Inc.*, No. 21-CV-58-CJCADSX, 2021 WL 3046775, at *2 (C.D. Cal. June 24, 2021) (dismissing CCPA claim because "Defendant's disclosure of Plaintiff's personal information ... was not caused by Defendant's failure to implement reasonable security procedures and practices"), *aff'd*, No. 21-55753, 2023 WL 334015 (9th Cir. Jan. 20, 2023); *McCoy v. Alphabet, Inc.*, No. 20-cv-05427-SVK, 2021 WL 405816, at *8 (N.D. Cal. Feb. 2, 2021) (dismissing CCPA claim because "there are no allegations of a security breach"); *Rosado v. Zuckerberg*, No. 1:21-cv-07840 (ALC), 2023 WL 5918055, at 3–4 (S.D.N.Y. Sept. 11, 2023) (dismissing CCPA claim in part because plaintiff alleged no "facts to support the contention that his information was subject to a data breach").[3]

This Court's decision in *Gershfeld*—affirmed by the Ninth Circuit—is particularly instructive. In *Gershfeld*, the plaintiff purchased a subscription to the defendant's software and was required to provide his name as well as his credit card number, expiration date, and verification code. 2021 WL 3046775, at *1. The defendant then allegedly renewed the subscription without plaintiff's authorization by disclosing plaintiff's private credit card information to the defendant's credit card processor. *Id*. As in the instant case, however, the alleged disclosure did not result from a security breach, and for this reason, this Court dismissed the CCPA claims with prejudice, stating:

[3] *See also* AB 375 (Chau and Hertzberg), Assembly Committee on Privacy and Consumer Protection, June 27, 2017, Appendix Tab 1 at 6 (describing the "limited private right of action for data breaches"); Office of the Attorney General, *California Consumer Privacy Act (CCPA)*, Appendix Tab 3 at 3, State of California Department of Justice, https://oag.ca.gov/privacy/ccpa ("You cannot sue businesses for most CCPA violations. You can only sue a business under the CCPA if there is a data breach, and even then, only under limited circumstances."); E-Commerce & Internet Law § 27.08[10][A] (2020) Appendix Tab 4 at 26-549 ("private right of action created by the CCPA may be brought only for data breaches").

> [T]o succeed on a CCPA claim, a plaintiff must allege that his personal information was subject to "unauthorized ... disclosure as a result of" a business's failure "to implement and maintain reasonable security procedures and practices." Plaintiff has not made such an allegation here.
>
> Plaintiff alleges that Defendant stored his personal information "in a nonencrypted and nonredacted fashion," but the disclosure of Plaintiff's personal information was not *caused by* this practice.

Id. at *2 (emphasis added) (citation omitted).

Here, Plaintiffs follow the *Gershfeld* playbook to the same result. While they recite in conclusory fashion that the MTB Defendants failed to implement, uphold, or maintain reasonable security procedures and practices (FAC ¶¶ 54, 72), the alleged facts supporting that conclusion state nothing of security procedures or practices. *See Iqbal*, 556 U.S. at 678–81 ("[t]hreadbare recitals of the elements of a cause of action" fail to state a claim). The FAC alleges only—and without any support[4]—that Plaintiffs' personal information was stored, transmitted, or disclosed "in a nonencrypted and nonredacted form." FAC ¶ 137. But even if that were true, Plaintiffs' claims still fail because Plaintiffs do not allege that the MTB Defendants' productions were "the result of" or "caused by" any security failure or cybersecurity breach.[5] *Gershfeld*, 2021 WL 3046775 at *2.

[4] Indeed, Plaintiffs' own evidence and allegations contradict any assertion that the MTB Defendants lacked appropriate security measures. As outlined above, Plaintiffs themselves allege that security measures were in place for the transfer of data pursuant to the subpoenas, specifically that "[t]he data is to be delivered electronically to the Arizona Attorney General's Office by delivery to its 'SFTP' (Secure File Transfer Protocol) site." FAC ¶ 60. Plaintiffs also allege that Defendant Western Union made payments to TRAC "to fund privacy, confidentiality, and *information security measures*" (*id.* ¶ 35 (emphasis added)), and that Forcepoint's product design assisted in "preserving the custody, *security*, and physical ownership of the data" (*id.* ¶ 97 (emphasis added)). These allegations highlight efforts made by the parties to *strengthen* security measures and contradicts § 1798.150's requirement that there was some failure of duty to implement safeguards.

[5] Forcepoint escapes liability under the CCPA for the same reason. The FAC is devoid of any allegations that the disclosures were the result of Forcepoint's failure "to implement and maintain reasonable security procedures and practices." *Gershfeld*, 2021 WL 3046775, at *2. To the contrary, the FAC alleges that Forcepoint was retained by TRAC for the specific purposes of providing "access" and "disclosure" of the underlying data to law enforcement officers, agents, or investigators. FAC ¶¶ 39–44, 79–81.

Plaintiffs' real concern is not a failure of security practices, but rather that they were not told in advance that information concerning their money transfers would be disclosed to law enforcement. *See* FAC ¶¶ 55–58, 73–76. In fact, the MTB Defendants consistently disclosed to all customers that their information could or would be disclosed to law enforcement or in response to government subpoenas. *See infra* Part IV.D.2. But even accepting Plaintiffs' contentions regarding the productions as true, the CCPA has separate provisions that govern a business's obligations to provide notice of and abide by its stated data collection and processing and sharing practices. *See, e.g.*, Cal. Civ. Code § 1798.100(a) (notice requirements), § 1798.100(c) (limitations on use and sharing to the notice provided), §1798.130(a)(5) (requiring online disclosures that include types of collected information and categories of third parties to whom it is disclosed). None of those provisions is within the scope of the CCPA's private right of action. *See* Cal. Civ. Code § 1798.150(c).

Plaintiffs do not allege any data breach or other security failure. They therefore failed to allege facts supporting a private right of action under the CCPA, and for that reason, this Court should dismiss Plaintiffs' CCPA claim with prejudice.

2. The CCPA Does Not Restrict A Business's Ability To Comply With Subpoenas.

Plaintiffs' CCPA claim also fails because Plaintiffs themselves expressly allege that the MTB Defendants produced transaction records in response to compulsory subpoenas. *See* FAC ¶¶ 45, 48, 59–60, 62–65. Section 1798.145 of the CCPA is clear: "the obligations imposed on businesses by [the CCPA] shall not restrict a business's ability to" comply with "federal, state, or local laws" or "a civil, criminal, or regulatory inquiry, investigation, ***subpoena***, or summons by federal, state, or local authorities." (Emphasis added).[6]

[6] *See also* AB 375 (Chau and Hertzberg), Senate Judiciary Committee, June 26, 2018 Appendix Tab 2 at 8 ("This bill would make clear that the obligations imposed on businesses by the Act do not restrict a business's ability to comply with the law or lawful orders; cooperate with law enforcement agencies concerning unlawful conduct or activity ….").

For the reasons discussed above, Plaintiffs are not saved from CCPA's statutory exception for compliance with compulsory subpoenas by their allegation that the subpoenas are somehow "facially invalid," or that the MTB Defendants "knew or should have known" that the subpoenas were invalid based on the Arizona Court of Appeals 2007 opinion in *Goddard*. *See supra* at Part IV.B. Nor can Plaintiffs plead around this exemption by alleging that the data in question was remitted to TRAC or Forcepoint, rather than directly to law enforcement. *See, e.g.*, FAC ¶ 66. The statutory exemptions by their plain terms do not require disclosure to any particular entity; rather, the exemptions preclude liability for *compliance* with the terms of the subpoenas at issue here. *See* Cal. Civ. Code § 1798.145. Indeed, the FAC alleges that the subpoenas "requested" and/or "required" the MTB Defendants to remit the requested data directly to TRAC and Forcepoint. FAC ¶¶ 45, 63.

Moreover, the FAC directly contradicts the notion that the data was not intended for law enforcement. As discussed above, the exemplar subpoena excerpted in paragraph 60 and attached in full as Exhibit A to the FAC was issued by the Arizona Attorney General, and states in no uncertain terms that "[t]he data is to be delivered electronically *to the Arizona Attorney General's Office* by delivery to *its* 'SFTP' (Secure File Transfer Protocol) site." Dkt. 30-1 (Ex. A to FAC) at 1 (emphasis added). There is no mention of TRAC in the subpoena, and Forcepoint is only identified as an "agent" of the Arizona Attorney General to assist with the data delivery. *Id.* at 1–2. The MTB Defendants' compliance with these subpoenas therefore clearly falls within CCPA's exemptions, and Plaintiffs' CCPA claim should be dismissed with prejudice.

Nor can Forcepoint's conduct be violative of the CCPA where it was used as a conduit of the Arizona Attorney General. The FAC alleges that Forcepoint was merely a software vendor engaged to develop a system to manage the data collected by law enforcement, without any responsibility, authority or control over how that data was used or shared. FAC ¶¶ 39–44. An individual affiliated with Forcepoint is identified in

the subpoena to provide "the secure VPN address" and data formatting assistance, and is identified as the Arizona Attorney General Office's "agent." Dkt. 30-1, (Ex. A to FAC), at 1–2. Given that the CCPA does not restrict a business's ability to comply with government subpoenas, it also cannot restrict an alleged "agent" from the same conduct.

Stated plainly, there was no cybersecurity breach or other security failure resulting in disclosure of the data at issue. Because any amendment is futile or would be subject to dismissal, Plaintiffs' CCPA claim should be dismissed with prejudice. *Carrico v. City and Cty. of San Francisco*, 656 F.3d 1002, 1008 (9th Cir. 2011).

D. Plaintiffs' California Constitutional Claim Should Be Dismissed Under Rule 12(b)(6) For Failure To State A Claim.

The California Constitution provides individuals with a qualified right of "privacy." Cal. Const., art. I, § 1. "[T]he California Constitution sets a 'high bar' for establishing an invasion of privacy claim." *Guilfoyle v. Beutner*, No. 2:21-cv-05009-VAP (MRWx), 2021 WL 4594780, at *21 (C.D. Cal. Sept. 14, 2021) (quoting *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1038 (N.D. Cal. 2014)). This privacy right is "not absolute," and often times "must yield to other important interests." *Grafilo v. Soorani*, 41 Cal. App. 5th 497, 507 (2019). Thus, to state a viable claim, a plaintiff must adequately allege three threshold elements to avoid dismissal: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy under the circumstances; and (3) conduct by the defendant that is so serious in nature, scope, and actual or potential impact as to constitute an egregious breach of the social norms. *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 287 (2009). A defendant may defeat a constitutional privacy claim by either "negating any of the three elements." *Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal. 4th 1, 40 (1994).

Even accepting all facts pleaded in the FAC as true, Plaintiffs' claim fails each element. Plaintiffs voluntarily provided their transaction data to the MTB Defendants

while on notice that the MTB Defendants might produce that data to governmental authorities, including law enforcement, pursuant to government subpoenas.

1. Plaintiffs Fail To Plead A Legally Protected Privacy Interest.

While Plaintiffs outline certain categories of information subpoenaed from the MTB Defendants, the FAC is silent as to what information Plaintiffs actually provided in the course of their transactions. *See* FAC ¶¶ 116–20. Courts do not acknowledge a cognizable privacy interest in every manner of consumer data, only that which is sufficiently sensitive and confidential. *Hill*, 7 Cal. 4th at 35; *see, e.g.*, *420 Caregivers, LLC v. City of L.A.*, 219 Cal. App. 4th 1316, 1349 (2012) (explaining that one's name, address, and phone number are "nonintimate in nature"); *In re Yahoo Mail Litig.*, 7 F. Supp. 3d at 1040 (no legally protected privacy interest in email generally); *Folgelstrom v. Lamps Plus, Inc.*, 195 Cal. App. 4th 986, 989 (2011) (expressing skepticism that a customer has a legally protected privacy interest in one's address). By failing to identify what information the individual Plaintiffs actually provided, the FAC cannot demonstrate that a legally protected privacy interest is at issue. *See Hayden v. Retail Equation, Inc.*, No. 8:20-cv-01203-JWH-DFMx, 2021 WL 5024502, at *6 (C.D. Cal. July 6, 2021) (dismissing constitutional privacy claim where complaint describes categories of information that *may* be included in a collection, but not what was actually collected); *Zbitnoff v. Nationstar Mortg.*, LLC, No. C 13-05221 WHA, 2014 WL 1101161, at *4 (N.D. Cal. Mar. 18, 2014) (dismissing constitutional privacy claim for failure to specify exactly what private information was collected in applying for mortgage and disclosed to third parties performing credit checks); *In re Yahoo Mail Litig.*, 7 F. Supp. 3d at 1041 (recognizing potential for sufficiently private information to be contained in email communications, but dismissing constitutional privacy claim for failure to plead what specific information was actually present).

2. Plaintiffs Had No Reasonable Expectation Of Privacy Against Production Of Their Transaction Data To Law Enforcement In Response To Government Subpoenas.

The "extent of a privacy interest is not independent of the circumstances." *Hill*, 7 Cal. 4th at 36 (cleaned up). Whether an objectively reasonable expectation of privacy exists must take into consideration (i) the "customs, practices, and physical settings" that attended customers' use of the MTB Defendants' services, and (ii) the "advance notice[s]" affirmatively and routinely provided to customers regarding how and when a company shares the information it collects—including to comply with law enforcement requests. *Id*. at 9, 36.

First, the voluntary disclosure of data to a money transfer business by customers wanting to transfer money (as here) always carries the potential that such data will be provided to law enforcement. The Supreme Court identified this construct as a common facet of doing business in modern society: a customer of a financial institution always assumes "the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government." *United States v. Miller*, 425 U.S. 435, 442–43, 445 (1976). For that reason, the Court held that there is no expectation of privacy in bank transaction records for purposes of the Fourth Amendment.[7] *Id.* Courts in the Ninth Circuit commonly agree. *See KRL v. Moore*, No. CIVS992437DFLDAD, 2006 WL 548520, at *5 (E.D. Cal. Mar. 3, 2006) (no legitimate expectation of privacy in bank records), *aff'd in part, rev'd in part on other grounds and remanded sub nom.*, *KRL v. Est. of Moore*, 512 F.3d 1184 (9th Cir. 2008); *United States v. Galloway*, No. 1:14-cr-00114-DAD-BAM, 2017 WL 735730, at *5 (E.D. Cal. Feb. 24, 2017) (no reasonable expectation of privacy over tax documents obtained from defendant's accountant because "one does not have a reasonable expectation of privacy in

[7] Though a different constitutional basis, the "reasonable expectation of privacy" test is fungible. *See, e.g.*, *Kamalu v. Walmart Stores, Inc.*, No. 1:13-CV-00627-SAB, 2013 WL 4403903, at *4 (E.D. Cal. Aug. 15, 2013) (applying Fourth Amendment precedent in context of California Constitutional privacy analysis).

information revealed to a third party which is passed on to the government"), *aff'd*, 802 F. App'x 247 (9th Cir. 2020); *United States v. Forrester*, 512 F.3d 500, 509 (9th Cir. 2008) (society not prepared to recognize a reasonable expectation of privacy in information voluntarily turned over to third parties). Indeed, simply contending that Plaintiffs "did not consent to [subpoena compliance], without more, does not support a reasonable expectation of privacy." *D'Angelo v. FCA US, LLC*, No. 3:23-CV-00982-WQH-MMP, 2024 WL 1625771, at *17 (S.D. Cal. Mar. 28, 2024); *see also*, *e.g.*, *In re Yahoo Mail Litig.*, 7 F. Supp. 3d at 1041 (rejecting the argument that "an allegation of lack of consent suffices to state a privacy claim").

Second, the MTB Defendants *did in fact* put customers on notice of potential sharing of data with law enforcement, directly diminishing any expectation of privacy. The FAC is littered with allegations that the MTB Defendants failed to disclose to their customers that their personal and transactional information could be shared or disclosed in response to the subpoenas at issue. *See*, *e.g.*, FAC ¶¶ 9, 55–58, 73–76, 111–12, 116–120, 150, 152. But while Plaintiffs cited certain disclosures to allegedly establish an expectation that their data would not be shared, *e.g.*, *id.* ¶¶ 148–49, Plaintiffs opted not to attach the MTB Defendants' full disclosures to the FAC.[8] Instead, Plaintiffs cherry-picked portions of the MTB Defendants' websites that concern fraud prevention and transactional security, characterizing them as the Defendants' "commitment to the privacy of the services they provide." *Id.* ¶ 2 (embedding website screenshots). The full disclosures that each MTB Defendant provide to customers—incorporated by reference into the FAC and judicially noticeable—establish that their information could be produced to law enforcement.

Western Union. Western Union provides notice to its customers that Western Union may disclose transactional data to the government in both its Terms and

[8] The FAC does not include any similar allegations concerning Forcepoint. In fact, Forcepoint did not interact with Plaintiffs at all; it was merely a software vendor who provided analytics for the TRAC database. FAC ¶¶ 79, 82, 97.

Conditions and in its Privacy Policy, both of which are available on its website,[9] including during the period (2020 through 2022) when Plaintiffs Guzman and Meza allege they transacted with Western Union. *See* FAC ¶¶ 116–17; Armbrust Decl., Exs. 1–5. Western Union's Terms and Conditions include a "Privacy" paragraph, which states that Western Union "may collect and disclose personal information to third parties as explained in [its] Privacy Statement," including "financial data (e.g., information on transactions with us and other financial matters), contact information, identification, computer, mobile device and social network information," and "[r]ecipients may include ... government agencies." Armbrust Decl., Exs. 1–3. Western Union's Privacy Statement similarly states that Western Union may "disclose [consumers'] personal information globally, as required or permitted by applicable laws and regulations, to regulatory and financial authorities, credit reporting agencies, law enforcement bodies, courts, governments, or government agencies to meet compliance and legal obligations." Armbrust Decl., Exs. 4–5.[10]

Additionally, Plaintiff Meza's signed receipt from her September 10, 2022 in-person transaction includes an acknowledgement (in both English and Spanish) that she "received and agreed to abide by" Western Union's Terms and Conditions, Dkt. 71-1, and the same Terms and Conditions that appear on Western Union's website were printed, in English and Spanish, on the back of the receipt she received. Dkts. 47-6, 47-7, ¶ 9. The back of the receipt also references Western Union's Privacy Policy. *Id.* Likewise, the registration and review pages that Plaintiff Guzman would have encountered when sending money transfers online or through the mobile application

[9] *Online Money Transfer Terms & Conditions*, Western Union, https://www.westernunion.com/us/en/legal/terms-conditions.html (last visited Nov. 22, 2024); *Western Union's Global Privacy Statement*, Western Union, https://www.westernunion.com/global/en/privacy-statement.html (last visited Nov. 22, 2024).

[10] This Court may take judicial notice of the contents of web pages available through the Internet Archive's Wayback Machine. *See* RJN at 6-7 (citing cases).

directly link, in blue font, to the Terms and Conditions and Privacy Policy. Dkt. 47-3 at 2, 4, 5, 7 (screenshots of the website and mobile transaction flow).[11]

MoneyGram. MoneyGram provides its customers with similar notice that data collected from money transfer customers may (or will) be shared with law enforcement. MoneyGram publishes clear privacy notices online identifying law enforcement as a recipient of customer data, incorporates notice of potential law enforcement disclosures directly into the terms and conditions for all money transfers, and prints a similar notice on the receipt for every in-person transaction.

Plaintiff Jimenez *himself* attached a copy of one such receipt to his previously filed Declaration in Support of Plaintiffs' Opposition to Defendants' Motion to Compel Arbitration (Dkt. Nos. 64, 65).[12] The receipt includes (just below the transaction information) the same disclosure quoted above, and then repeats it in Spanish. Dkt. No. 65, at 3. The FAC's mischaracterizations of MoneyGram's disclosures are contradicted by the direct disclosure document retained by Plaintiff Jimenez himself, and submitted to this court as evidence. The Jimenez receipt clearly states—in English and Spanish just below the transaction information—that "MoneyGram may disclose your personal information to third parties," lists precisely the types of information sought by the Arizona AG subpoenas, and states that it may be provided to "governmental or other regulatory agencies (including law enforcement officials within or outside the United

[11] As explained in Defendants' Request for Judicial Notice, the Court does not need to take judicial notice of documents (including declarations and exhibits) previously filed in this action, but in any event, these documents are proper subjects of judicial notice and are incorporated by reference. *See* RJN at pg. 8-10 (citing cases).

[12] The Court "need not take judicial notice of previously filed documents in this action." *Medina v. Circle K Stores, Inc.*, No. EDCV22557JGBKKX, 2022 WL 16966534, at *2, n.1 (C.D. Cal. Sept. 7, 2022) (declaration previously filed in the same action considered in assessing motion to dismiss for failure to state a claim); *see also Acosta v. City of Chino*, No. CV 18-914 DSF (KKX), 2021 WL 9700611, at *4 (C.D. Cal. Sept. 1, 2021) (granting judicial notice request but advising for future reference that parties "*need not seek judicial notice of documents previously filed in the same case.* An accurate citation will suffice.") (emphasis added). If necessary, however, this exhibit would certainly qualify for judicial notice, as its authenticity is beyond dispute—Plaintiff himself authenticated it—and it is being offered not for its truth but for the notice it provided. *See* RJN at 8-10.

States)." *Id.* As part of the same disclosure, Mr. Jimenez's proffered receipt also includes a URL to access MoneyGram's "Privacy Statement and practices with respect to your personal information at www.moneygram.com/privacy-notice," which links to the MoneyGram's online Global Privacy Notice discussed in greater detail, below. *See* Declaration of Christopher James in support of Defendants' Motion to Dismiss FAC ("James Decl."), ¶10.

In-person customers receive similar notices in MoneyGram's Terms and Conditions, which are presented to all customers in print and incorporated in electronic form throughout the transaction process.[13] The Terms and Conditions include a stand-alone section titled "Privacy Notice" stating "MoneyGram may disclose your personal information to third parties, [including] your contact information, your identification, information about the Transfer or your use of the Services, or other information relating to financial matters. The information may be disclosed to … governmental or other

[13] As explained in detail in MoneyGram's previously filed Motion to Compel Arbitration (Dkt. 42-1), and Declaration of Jessica Kelly in Support of MoneyGram's Motion to Compel Arbitration and Stay Proceedings ("Kelly Arbitration Decl.") (Dkt. 42-2), the in-person transaction flow presented these Terms (in English and Spanish) via (i) an initial "Send Form" that preceded the transaction and collected the relevant customer information; (ii) clearly and conspicuously incorporated the Terms by reference into a "Confirmation Form" signed by the customer that acknowledged the application of the Terms to the transaction (and provided a URL to an online version); (iii) a "Customer Receipt" at the conclusion of the transaction, similarly acknowledging the applicable terms and incorporating them with an online URL; and (iv) a "Receipt Jacket" with another physical printed copy of the full Terms. *See* Kelly Arbitration Decl. ¶¶8-14, Exs. A-K (Dkt. . Given the FAC's extensive citation to the customer disclosures and reliance upon them in support of Plaintiff's causes of action, the in-person transaction documents submitted in the Kelly Arbitration Declaration are incorporated by reference into the FAC, and appropriately considered by this Court on a motion to dismiss. *See* RJN, at 8.

Moreover, Kelly Arbitration Decl. Exhibits D-1 through D-6 are copies of Confirmation Forms that include Plaintiff Jimenez' physical signature, which Mr. Jimenez himself verified and authenticated by declaration in opposition to MoneyGram's motion to compel arbitration. Dkt. 64, ¶12. As these documents are not offered for the truth of their contents, but rather for the notice they provided to Plaintiff and others like him, and their authenticity is beyond dispute (Mr. Jimenez authenticated them himself), they are appropriate for judicial notice by the Court and consideration here. *See* RJN at 8-10. The Confirmation Forms acknowledge receipt of the Terms, including the Privacy Notice quoted above, and in multiple instances incorporate the online version of Terms by reference, via a conspicuous URL that appears immediately above Mr. Jimenez's signature. Kelly Arbitration Decl., Ex. D-3, D-4 (Dkt. 42-6).

regulatory agencies (including law enforcement officials within or outside of the United States)." *See* James Decl., ¶11, Ex. 6 (offered in both English and Spanish).[14]

MoneyGram's online privacy disclosures are entirely consistent. The FAC blatantly mischaracterizes MoneyGram's privacy notices by embedding a screenshot from within MoneyGram's online "Help Center" section on "fraud prevention" to support its claims that MoneyGram never disclosed that customer information could be reported to law enforcement. ¶2, fn. 2 (making no mention of privacy issues). It is unclear why Plaintiffs chose to incorporate a screenshot from this inapplicable page, rather than the site's clearly labeled "Privacy Center" (accessed by hyperlink from MoneyGram's homepage in close proximity to the Help Center hyperlink Plaintiffs chose instead). James Decl., ¶6. The Privacy Center includes Global Privacy Notices in more than thirty languages, as well as specific privacy notices for the United States and California Residents.[15] These privacy notices each disclose the collection and sharing of customer data to law enforcement, and have consistently done so during the FAC's relevant period. *See* James Decl., ¶¶8-9, Exs. 3-5.

MoneyGram's "Global Privacy Notice" is also presented to all online users as part of MoneyGram's online account creation flow, bolded and underlined, providing conspicuous notice to all customers who register to use MoneyGram's online services. *See* James Decl. ¶7, Ex. B (screen captures of account creation and transaction process). The same notice is linked just before an online transaction is submitted, often called a "just-in-time notice" with language immediately above the "Submit Transaction" button that reads "You acknowledge your information will be used, disclosed and transferred, including international transfers as described in our **Privacy Notice**." *See Id.* (emphasis in original). The Global Privacy Notice identifies the various pieces of

[14] This, and other James Declaration exhibits that follow are publicly verifiable website captures, either of MoneyGram's website as it currently stands or during the FAC's relevant period, captured from Internet Archive Wayback Machine, and judicially noticeable. *See* RJN at 6-7.

[15] https://www.moneygram.com/intl/privacy-center (last visited Oct. 24, 2024).

customer and transaction information collected by MoneyGram (including those reflected in the subpoenas at issue, here), and provides notice in *three different places* that such information is shared with law enforcement in response to subpoenas. James Decl., ¶8, Ex. 3 (e.g., Under the heading "How We Share and Disclose Personal Information," the Global Privacy Notice discloses that MoneyGram "may . . . disclose Personal Information . . . [t]o comply with any court order, law, or legal process, including to respond to any government or regulatory request.")

U.S. Privacy Notices published in the FAC's relevant period and available throughout 2022 (the year of Mr. Jimenez's alleged MoneyGram transactions) provide notice that consumers have "the right to limit some but not all sharing" of personal information, and lists types of information collected (including government identification numbers, date of birth, contact information, transaction history, bank account information, and various internet-related data points). James Decl., ¶9 Exs. 4 and 5. The very first category of "[r]easons we can share your information" states: "For our everyday business purposes—such as to … cooperate with criminal or government investigations [and] respond to court orders and subpoenas." Two questions follow: (1) "Does MoneyGram share?" Answer: "Yes"; (2) "Can you limit this sharing?" Answer: "No." *Id.*

DolEx. DolEx also provides its customers with notice (through its website via its User Agreement and Privacy Policy[16], as well as in-person printed receipts) that data collected from money transfer customers may be shared with law enforcement or as permitted by law.

DolEx's User Agreement and Privacy Policy, translated in both English and Spanish, are currently found on its website, as well as during the time when Plaintiffs Carrillo and Perez allegedly used DolEx's services. *See* FAC ¶¶ 119–20; Declaration of Katherine L. Alphonso in Support of Defendants' Motion to Dismiss FAC

[16] *Privacy Policy*, https://www.dolex.com/legals/#privacypolicy (last visited November 25, 2024); *User Agreement*, https://www.dolex.com/legals/#useragreement (last visited November 25, 2024).

("Alphonso Decl."), ¶ 2, Exs. 1-2. The User Agreement, under Collection of Information, states in relevant part that DolEx "may provide information about [its customers and their transactions] to government authorities and enforcement agencies, as required by law and described in [its] Privacy Policy." *See* Alphonso Decl. ¶ 2, Ex. 2. The Privacy Policy, under Information Sharing, states in relevant part that DolEx "may disclose [customer] information . . . with third parties . . . pursuant to a subpoena, court order, government inquiry, or other legal process, or as otherwise required by law . . . ." *See* Alphonso Decl. ¶ 2, Ex. 1.

For customers transacting in-person, DolEx prints a receipt putting customers on notice of the possibility of DolEx disclosing personal information to third parties, including but not limited to law enforcement and/or government agencies, as well as referencing its Privacy Policy and other terms and conditions. In fact, Plaintiff Perez's signed receipts from his in-person transactions with DolEx, submitted as part of his declaration in support of Plaintiffs' Opposition to DolEx's Motion to Compel Arbitration, confirm the provided disclaimer, again in both English and Spanish, that "DolEx does not disclose any non-public, personal or financial information of customers to third parties, *except as permitted by law* . . . ." Dkt. 61 (emphasis added). The applicable receipts go on to inform him that he "may obtain a copy of [DolEx's] privacy policy and terms and conditions" from its website, an agent or branch location, or by calling a toll-free number. *Id*.

* * *

As is evidenced from the disclosures discussed above, the MTB Defendants' applicable privacy notices and policies expressly informed Plaintiffs that their data might be collected and disclosed to the government in the manner alleged. Plaintiffs therefore have no reasonable expectation of privacy against such productions, and their constitutional claim should be dismissed with prejudice. *See Hammerling v. Google, LLC*, No. 22-17024, 2024 WL 937247, at *3 (9th Cir. Mar. 5, 2024).

3. Plaintiffs Cannot Satisfy The Requirement That The MTB Defendants' Compliance With Law Enforcement Subpoenas Is So Serious In Nature, Scope, And Actual Or Potential Impact As To Constitute An Egregious Breach Of Social Norms.

Compliance with investigative subpoenas does not constitute "a serious invasion of privacy," as required to establish a constitutional privacy violation. *Hill*, 7 Cal. 4th at 39–40. It is hardly an "egregious breach of the social norms" for a company, presented with statutorily authorized subpoenas, to obey a state or federal law enforcement agency's demand for transaction data. *Id.* at 37; *cf. In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1063 (N.D. Cal. June 12, 2012) (disclosure of unique device identifier, personal data, and geolocation information not an egregious breach of social norms); *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1025 (N.D. Cal. 20212) ("Even disclosure of personal information, including social security numbers, does not constitute an 'egregious breach of the social norms' to establish an invasion of privacy claim."). This is particularly true where, as discussed above, Plaintiffs were given repeated notice that this precise form of disclosure could occur.

The notion that compliance with law enforcement subpoenas is generally recognized and accepted is codified across a spectrum of informational privacy laws that either affirmatively require, or expressly exempt from liability, the reporting of consumer data pursuant to law enforcement or government process. This includes, as discussed above, the Annunzio-Wylie Act, 31 U.S.C. § 5318(g)(3)(A), and the CCPA, Cal. Civ. Code § 1798.145. *See supra* at Parts IV.B, IV.C.2. It also includes the Arizona Criminal Code, pursuant to which the Arizona Attorney General subpoenas were issued, which explicitly bars "civil or criminal liability against such custodian or financial institution in any action brought alleging violation of the confidentiality of such records." Ariz. Rev. Stat. Ann. § 13-2315. Additionally, California's Financial Information Privacy Act (Cal. FIPA) includes multiple exceptions for reporting nonpublic personal information, including where required or permitted under law "or

for an investigation on a matter related to public safety," "to comply with a properly authorized civil, criminal, administrative or regulatory investigation or subpoena or summons by federal, state, or local authorities," or to "respond to judicial process." Cal. Fin. Code § 4056(b)(5), (7). *See also* Stored Communications Act, 18 U.S.C. § 2703(c)(2), (e) (providing immunity from suit for providing information in accordance with the terms of a court order, warrant, or subpoena). Federal and state legislatures' (including California's) recognition of the importance of subpoena compliance provides critical context that appropriately benchmarks a citizen's privacy interests against a company's duty to adhere to law enforcement demands.

Consistent with the relevant legislatures' judgment that subpoena responses are well within acceptable social norms, California courts regularly hold that legitimate government actions justify disclosures, even where a privacy interest may exist. *See Whitney v. Montegut*, 222 Cal. App. 4th 906, 919 (2014), *as modified* (Jan. 21, 2014) (affirming decision to compel response to investigative subpoenas). This deference extends to a broad range of law enforcement functions: "identifying and rectifying violations" of state and federal laws, *Tom v. Schoolhouse Coins, Inc.*, 191 Cal. App. 3d 827, 830 (Ct. App. 1987); reviewing corporate records to "protect the public" from crimes and statutory infractions, *Lewis v. Super. Ct.*, 3 Cal. 5th 561, 572 (2017); and issuing subpoenas "to fulfill [the state's] mandate to protect public health and safety," *Kirchmeyer v. Helios Psychiatry Inc.*, 89 Cal. App. 5th 352, 360 (2023), *as modified* (Mar. 15, 2023), *rev. denied* (May 31, 2023).

Here, as Plaintiffs allege, the MTB Defendants produced transactional data in response to compulsory governmental subpoenas. *See* FAC ¶¶ 45, 48, 59–60, 62–65. And as discussed above, Plaintiffs' conclusory challenges to the subpoenas as "unenforceable" and "facially invalid" do not change this analysis. *See supra* Part IV.B. *See, e.g.*, *Sams v. Yahoo! Inc.*, 713 F.3d 1175, 1181 (9th Cir. 2013) ("bald legal conclusions are not entitled to be accepted as true and thus do not suffice to prevail

over a motion to dismiss"). Again, Plaintiffs' only support for their allegations that the MTB Defendants "knew or should have known" that the subpoenas were "facially invalid" is *Goddard*, but that case involved distinct issues involving an easily distinguishable 2006 subpoena issued for different investigative purposes. *See supra* at Part IV.B. Plaintiffs have entirely failed to allege any facts to establish the invalidity of the present subpoenas, much less to establish that the MTB Defendants should have reached that conclusion when the subpoenas were issued.

In sum, as the Arizona Attorney General herself emphasized in her letter to the Court, Arizona's "success in combatting [] sophisticated [Transnational Criminal Organizations] is highly dependent on [her] ability to issue and enforce the subpoenas and obtain the requested transactional records" from the MTB Defendants. Armbrust Decl., Ex. 6 at 43; *see also* Dkt. 30-2 (Ex. B to FAC) at 1 (explaining that data provided to TRAC assists law enforcement in "their efforts to disrupt criminal organizations and dismantle their operations"). Plaintiffs' constitutional claim should be dismissed with prejudice.

V. CONCLUSION

For the foregoing reasons, Defendants respectfully request that this Court dismiss the FAC with prejudice.

Dated: November 25, 2024

VINSON & ELKINS LLP

By: /s/ *Christopher W. James*
Ephraim Wernick
Christopher W. James
Briana R. Falcon
Attorneys for Defendant MoneyGram Payment Systems, Inc.

///
///
///
///
///

Dated: November 25, 2024

SIDLEY AUSTIN LLP

By: /s/ *Sheila A.G. Armbrust*

Sheila A.G. Armbrust (SBN 265998)
sarmbrust@sidley.com
555 California Street
San Francisco, CA 94104
Telephone: (415) 772-7430

Jodi E. Lopez (SBN 231117)
jlopez@sidley.com
350 South Grand Ave.
Los Angeles, CA 90071
Telephone: (213) 896-6000

Hille R. Sheppard (*pro hac vice*)
Joseph R. Dosch (*pro hac vice*)
Andrew F. Rodheim (*pro hac vice*)
hsheppard@sidley.com
jdosch@sidley.com
arodheim@sidley.com
One South Dearborn
Chicago, IL 60603
Telephone: (312) 853-7000

Attorneys for Defendant
Western Union Financial Services, Inc.

Dated: November 25, 2024

DUANE MORRIS LLP

By: /s/ *Daniel M. Doft*

Courtney L. Baird (SBN 234410)
clbaird@duanemorris.com
865 South Figueroa Street, Suite 3100
Los Angeles, CA 90017-5450
Telephone: (619) 744-2200
Fax: (619) 744-2201

Aaron T. Winn (SBN 229763)
Daniel M. Doft (SBN 317204)
atwinn@duanemorris.com
ddoft@duanemorris.com
750 B Street, Suite 2900
San Diego, CA 92101
Telephone: (619) 744-2200

Attorneys for Defendant
FORCEPOINT LLC

Dated: November 25, 2024

KAUFMAN DOLOWICH, LLP

By: /s/ *Katherine L. Alphonso*

Tad A. Devlin (SBN 190355)
Marcus Dong (SBN 251723)
Katherine L. Alphonso (SBN 314926)
2100 California Street, Suite 2100
San Francisco, CA 94104
tdevlin@kdvlaw.com
mdong@kaufmandolowich.com
kalphonso@kaufmandolowich.com
Telephone: 415.926.7600

Attorneys for Defendant
DOLEX DOLLAR EXPRESS, INC.

I, Christopher W. James, attest that Sheila A.G. Armbrust of Sidley Austin, LLP, Daniel M. Doft of Duane Morris, LLP, and Katherine L. Alphonso of Kaufman Dolowich, LLP, have read and approved the MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF ALL DEFENDANTS' JOINT MOTION TO DISMISS FIRST AMENDED COMPLAINT and consent to its filing in this action, and to affixing their signatures to it.

/s/ Christopher W. James
Christopher W. James

CERTIFICATE OF COMPLIANCE

The undersigned, counsel of record for Defendant Moneygram Payment Systems, Inc., certifies that this brief contains 11,821 words, which complies with the word limit of the Order Granting Joint Stipulation Regarding Briefing Schedule and Word Counts for Defendants' Motion to Dismiss (Dkt. 91).

Dated: November 25, 2024

VINSON & ELKINS LLP

By: */s/ Christopher W. James*
Christopher W. James